corelight

Virtual Sensor

Flexible traffic visibility in a virtual form factor

The Corelight Virtual Sensor for Hyper-V is designed to go wherever you need it, analyzing network traffic at speeds of up to 8 Gbps.

Deploy in Hyper-V in 15 minutes
Successfully deploy Corelight Virtual Sensors in a few simple steps: download the image, activate the license key, and follow the installation wizard to set a handful of configuration parameters.

Focus on your traffic, not instances
The Corelight Virtual Sensor is designed with flexibility in mind so you can deploy the right sizes for your traffic needs. It's also conveniently licensed on capacity so you can spin up the instances needed for your environment and adjust them as your traffic evolves.

Next-level analytics
Behavioral analysis, machine learning, and signatures give Corelight customers comprehensive threat detection coverage across network vulnerabilities and attacks. The Corelight Labs team continuously validates our detections on live customer networks to ensure that the best analytic and machine learning models are used for a given security challenge. Continuous detection engineering from open source communities also gives Corelight customers crowd-sourced confidence to detect known threats and delivers immediate access to zero day detections.

Microsoft Hyper-V

The Corelight Virtual Sensor provides network traffic insights across a range of environments:

- In branch locations
- On manufacturing floors
- In remote offices
- In high-value enclaves

The features you wish open-source had

Corelight has merged the power of Zeek and Suricata with a suite of enterprise features that dramatically improve usability, like an intuitive management UI, flow shunting, sensor health metrics, fleet management, and automated data export to Splunk, Elastic, Kafka, Syslog, S3, and more.

Specifications

Best-in-class Zeek and Suricata deployment:

- Corelight's best-in-class Zeek and Suricata platform in a virtual machine
- Built-in Zeek packages for detection, monitoring, and data enrichment
- Intuitive, 15 minute configuration, with a beautiful web UI
- Capacity-based licensing model for deployment flexibility
- Zeek log export to Splunk, Elastic, Kafka, Syslog, SIEMs, and SFTP
- High performance and efficient file extraction
- Comprehensive REST API for configuration and monitoring
- Minimalist, custom OS optimized for secure operation
- Automatic updates and feature enhancements
- World-class support from the definitive Zeek experts

Hyper-V reference configurations:

Nominal capacity	vCPUs	RAM (GB)	Disk (GB)
500 Mbps	4	16	500
1 Gbps	8	32	500
2 Gbps	16	64	500
4 Gbps	32	128	1000
6 Gbps	48	192	2000
8 Gbps	64	256	4000

Hyper-V minimum system requirements

- Windows Server 2016 Hyper-V environment
- Online access for seeding (i.e., inserting certificate)

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497